CCDCOE

EVE & ADAM

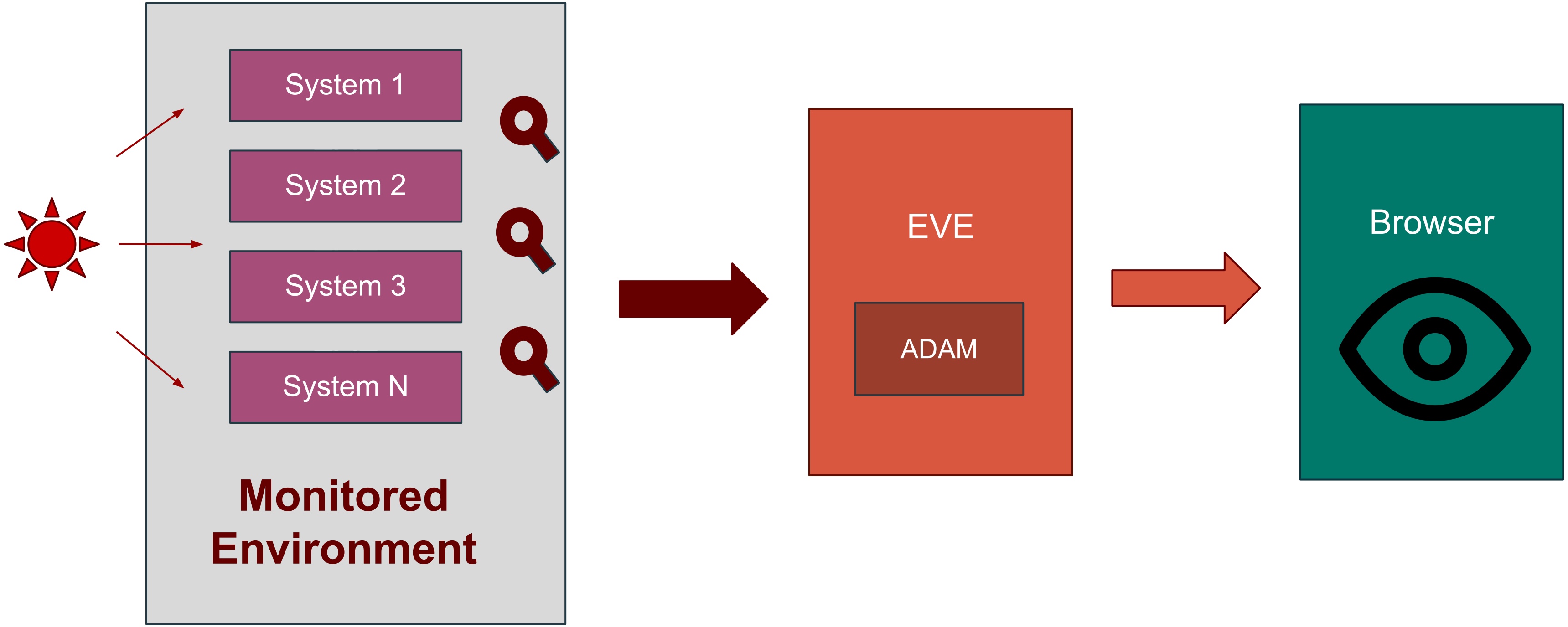
Situation Awareness Tools
for NATO CCDCOE Cyberexercises

F. Jesús Rubio. May 9, 2018.

Authors

- **Mauno Pihelgas**
  - NATO CCDCOE Researcher. Tallinn (Estonia).
- **Teemu U. Väisänen**
  - VTT Technical Research Center. Oulu (Finland). Former NATO CCDCOE Researcher.
- **F. Jesús Rubio Melón**
  - Spanish Joint Cyber Defence Command. Madrid (Spain). Former NATO CCDCOE Researcher

EVE and ADAM. An Overview



EVE & ADAM. Goals and Features

CCDCOE

- **Goals**:
  - Visualize Security Violation Attacks on Monitored Networks -> Situational Awareness
  - Complement existing Situational Awareness solutions (based on graphs and charting)
- **Features**:
  - Simple and Intuitive (even for decision makers!)
  - Not “too technical”
  - Valid in “mixed” environments (IT + CP systems)
  - Real time
  - Web interface

CCDCOE

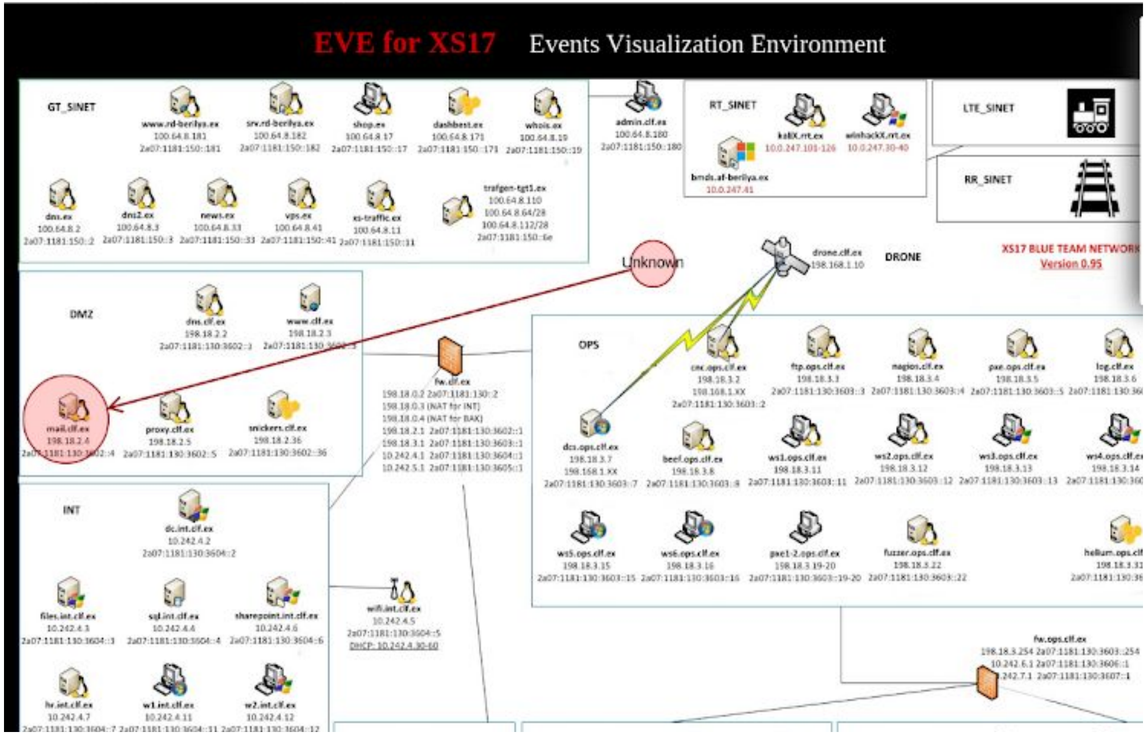
Our testing environment

- Tested on NATO CCDCOE Cyberexercises (“mimic real world”)
  - Crossed Swords
  - Locked Shields
- Mixed Environment
  - Traditional IT systems (Windows, Linux and Mac servers and workstations)
  - CP systems (SCADA, power grids)
- Heavy load attacks
- Multiple Monitoring Systems

Applicability

EVE can be applied to **any monitored environment**

EVE. A preview


EVE for XS17
Events Visualization Environment
GT_SINET
www.rd-berilya.ex 100.64.8.181 2a07:1181:150::181
srv.rd-berilya.ex 100.64.8.182 2a07:1181:150::182
shop.ex 100.64.8.17 2a07:1181:150::17
dashbest.ex 100.64.8.171 2a07:1181:150::171
whois.ex 100.64.8.19 2a07:1181:150::19
admin.clf.ex 100.64.8.180 2a07:1181:150::180
dns.ex 100.64.8.2 2a07:1181:150::2
dns2.ex 100.64.8.3 2a07:1181:150::3
news.ex 100.64.8.33 2a07:1181:150::33
vps.ex 100.64.8.41 2a07:1181:150::41
xs-traffic.ex 100.64.8.11 2a07:1181:150::11
trafgen-tgt1.ex 100.64.8.110 100.64.8.64/28 100.64.8.112/28 2a07:1181:150::6e
RT_SINET
kaliX.rt.ex 10.0.247.101-126
winhackX.rt.ex 10.0.247.30-40
bmds.af-berilya.ex 10.0.247.41
LTE_SINET
RR_SINET
Unknown
drone.clf.ex 198.168.1.10
DRONE
XS17 BLUE TEAM NETWORK
Version 0.95
DMZ
dns.clf.ex 198.18.2.2 2a07:1181:130:3602::3
www.clf.ex 198.18.2.3 2a07:1181:130:3602::3
mail.clf.ex 198.18.2.4 2a07:1181:130:3602::4
proxy.clf.ex 198.18.2.5 2a07:1181:130:3602::5
snickers.clf.ex 198.18.2.36 2a07:1181:130:3602::36
fw.clf.ex
198.18.0.2 2a07:1181:130::2
198.18.0.3 (NAT for INT)
198.18.0.4 (NAT for BAK)
198.18.2.1 2a07:1181:130:3602::1
198.18.3.1 2a07:1181:130:3603::1
10.242.4.1 2a07:1181:130:3604::1
10.242.5.1 2a07:1181:130:3605::1
OPS
cnc.ops.clf.ex 198.18.3.2 198.168.1.XX 2a07:1181:130:3603::2
ftp.ops.clf.ex 198.18.3.3 2a07:1181:130:3603::3
nagios.clf.ex 198.18.3.4 2a07:1181:130:3603::4
pxe.ops.clf.ex 198.18.3.5 2a07:1181:130:3603::5
log.clf.ex 198.18.3.6 2a07:1181:130:36
dcs.ops.clf.ex 198.18.3.7 198.168.1.XX 2a07:1181:130:3603::7
beef.ops.clf.ex 198.18.3.8 2a07:1181:130:3603::8
ws1.ops.clf.ex 198.18.3.11 2a07:1181:130:3603::11
ws2.ops.clf.ex 198.18.3.12 2a07:1181:130:3603::12
ws3.ops.clf.ex 198.18.3.13 2a07:1181:130:3603::13
ws4.ops.clf.ex 198.18.3.14 2a07:1181:130:36
ws5.ops.clf.ex 198.18.3.15 2a07:1181:130:3603::15
ws6.ops.clf.ex 198.18.3.16 2a07:1181:130:3603::16
pxe1-2.ops.clf.ex 198.18.3.19-20 2a07:1181:130:3603::19-20
fuzzer.ops.clf.ex 198.18.3.22 2a07:1181:130:3603::22
helium.ops.clf 198.18.3.31 2a07:1181:130:36
INT
dc.int.clf.ex 10.242.4.2 2a07:1181:130:3604::2
files.int.clf.ex 10.242.4.3 2a07:1181:130:3604::3
sql.int.clf.ex 10.242.4.4 2a07:1181:130:3604::4
sharepoint.int.clf.ex 10.242.4.6 2a07:1181:130:3604::6
wifi.int.clf.ex 10.242.4.5 2a07:1181:130:3604::5 DHCP: 10.242.4.30-60
hr.int.clf.ex 10.242.4.7 2a07:1181:130:3604::7
w1.int.clf.ex 10.242.4.11 2a07:1181:130:3604::11
w2.int.clf.ex 10.242.4.12 2a07:1181:130:3604::12
fw.ops.clf.ex
198.18.3.254 2a07:1181:130:3603::254
10.242.6.1 2a07:1181:130:3606::1
.242.7.1 2a07:1181:130:3607::1

Key Elements

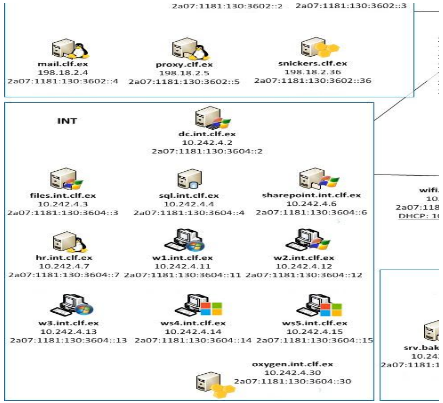
- Network Map
- The sensors
- JSON Messages
- Events & Alerts
- Kafka
- ADAM

The Network Map

CCDCOE

- ❖ *Represents* the monitored environment
- ❖ It it the underlying background of the web app.
- ❖ It does not have to be “real”.
  - ➢ Just a meaningful representation

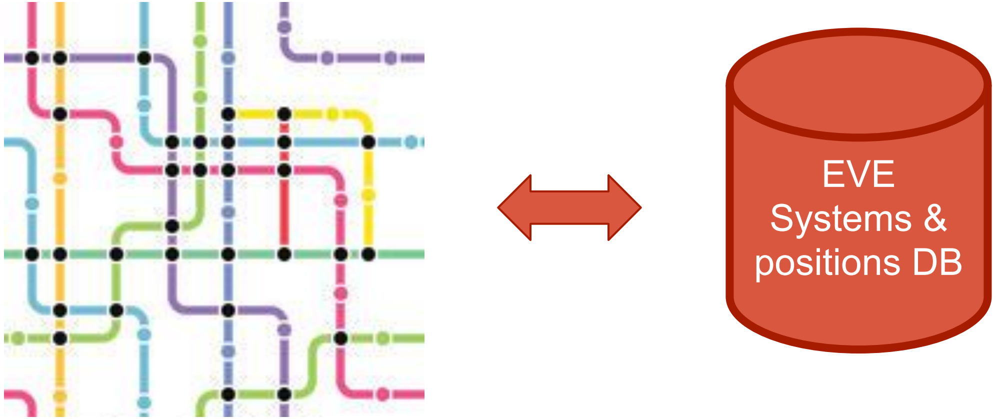
Neumáticos
Motor
Carrocería
Alumbrado
Automóvil
Volante
Espejos retrovisores
Asientos
Cambio de marchas
Salpicadero



Drawing on the Network Map

How is it possible to **draw alerts on the right position**?

- ➢ EVE keeps a database that correlates systems and their coordinates.
- ➢ That information has to be preloaded before EVE is used!



EVE
Systems &
positions DB

Static or Dynamic Network Map?

CCDCOE

- Why a dynamic network map?
  - Network maps need not be (fully) known.
  - Monitoring leads to discovery of possibly unknown hosts or devices
- Problems with dynamic network maps (our own experience):
  - Little info at the beginning (no “big picture”)
  - Harder to display (is it a server, an HMI interface, workstation??)
  - Harder to …
- Our experience: not so good so far...
- EVE uses static maps
- Future work: “Mixed” maps: static and dynamic content

The Sensors

- IDS or IPS (Suricata, Snort, Bro, …)
- Event Logs (Snoopy)
- Honeypots
- SIEM systems (Alient Vault, OSSIM, ELK - Elastic Search/Logstash)

The JSON messages

Message from the sensors to EVE:

```
{
    "source”  : {
        "IPV4"          :   "192.168.8.17" ,
        "IPV6"          :   ""
    } ,

    "target”  : {
        "type "         :   "host” ,
        "IPV4"          :   "” ,
        "IPV6"          :   "fe80:1181:150::33/64” ,
        "name"          :   "hostX”
    } ,

    "payload” : {
        "name”          :   "SQLi” ,
        "sensor”        :   "IDS” ,
        "evidence”      :   "SQL command 'or 1=1' found in URL” ,
        "url”           :   "http://www.example.com/query”
   } ,
}
```

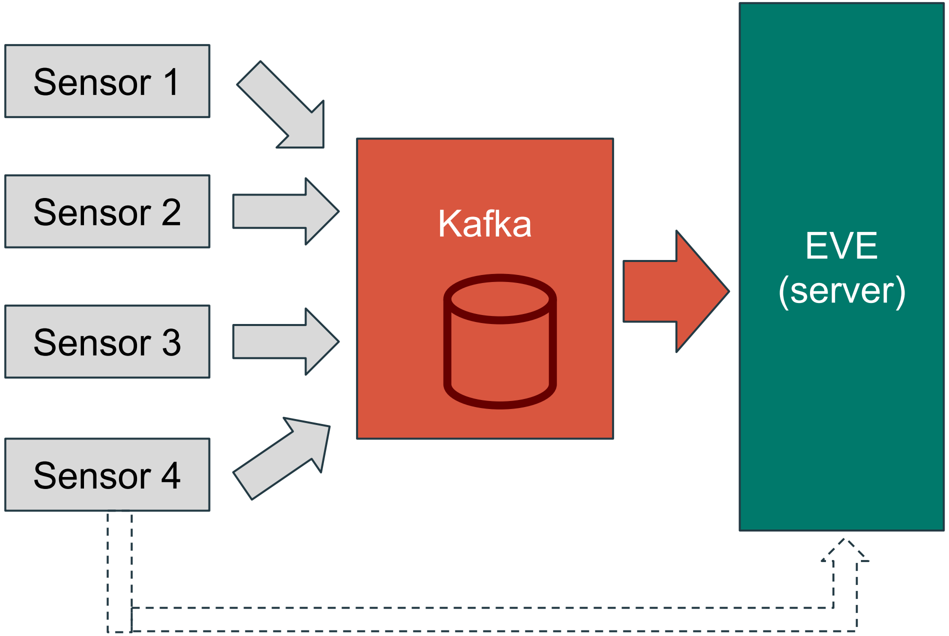
Events and Alerts

- **Events**: security violation attack detected by a sensor
- **Equivalent events**: two events are equivalent if they share
  - source
  - target
  - payload
  - within a given time frame
- **Alert**: the set of all equivalent events to any given event.
  - EVE´s goal: draw alerts (not events) on a network map

Kafka Streams

- Direct communication Sensors -> EVE ??
  - Lost connections problems
  - Data loss
  - Database required

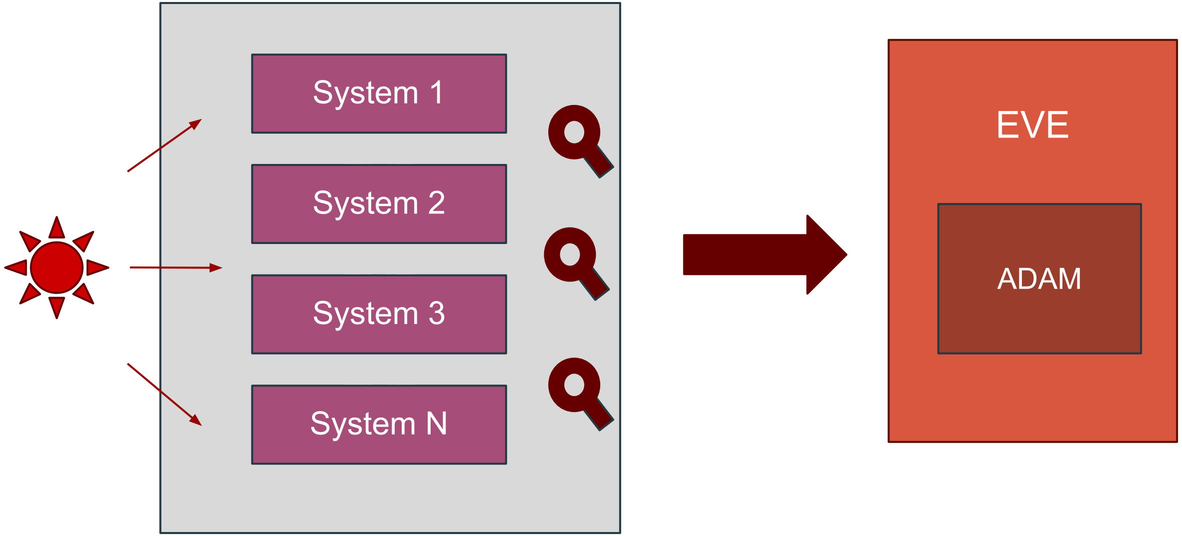
- Our solution: Kafka Streams
  - Communication Sensors <-> Kafka <-> EVE



ADAM

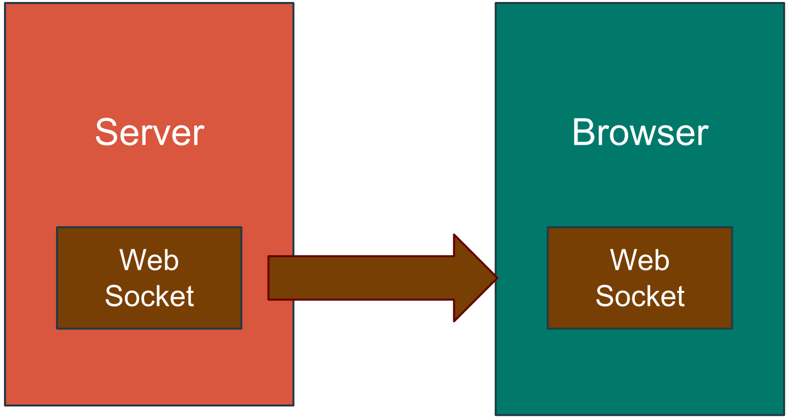
CCDCOE

- **Events correlator**/aggregator. It combines the events to generate the alerts
  - Different sensors may report the same attack
  - A given sensor may report the same attack at different times



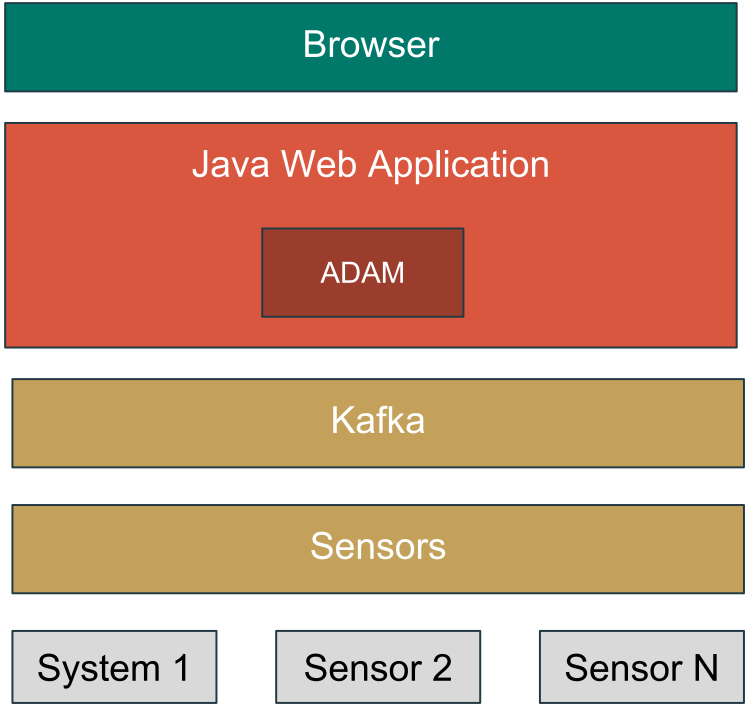
EVE Web Technology

- Java Web Application
  - JDK 8
  - Tomcat 8.5
- JavaScript + AJAX
  - Fast client-side drawing
- Web sockets
  - Real-time rendering
  - Avoids page reloading



EVE & ADAM. Full Stack

CCDCOE



Browser

Java Web Application

ADAM

Kafka

Sensors

System 1

Sensor 2

Sensor N

EVE & ADAM. Key facts

A Situational Awareness Tool:

1. **Less is more**: clarity, simplicity are mandatory
2. **Based on the right “network map”**: any meaningful representations of your CP systems
3. **Complimentary**: Compliments and enhance existing Situational Awareness solutions.

An alternative approach: mapping

Use map technology (layered representation) as base technology

- Advantages:
  - Zoom in/out capabilities
  - Reuse existing software
- Network map is base layer
  - Note: It does not need to be a “cartographic map”
- Attacks/Alerts become temporary layers on top of base layer

CCDCOE

Thank you!. Any Question?

F. Jesús Rubio
jrubio@isdefe.es